How to View Remediation Effort for Findings in Audit Workbench

This page has been made public for vendors

Question

How do I view the remediation effort assigned by Fortify for the findings reported in my scan?

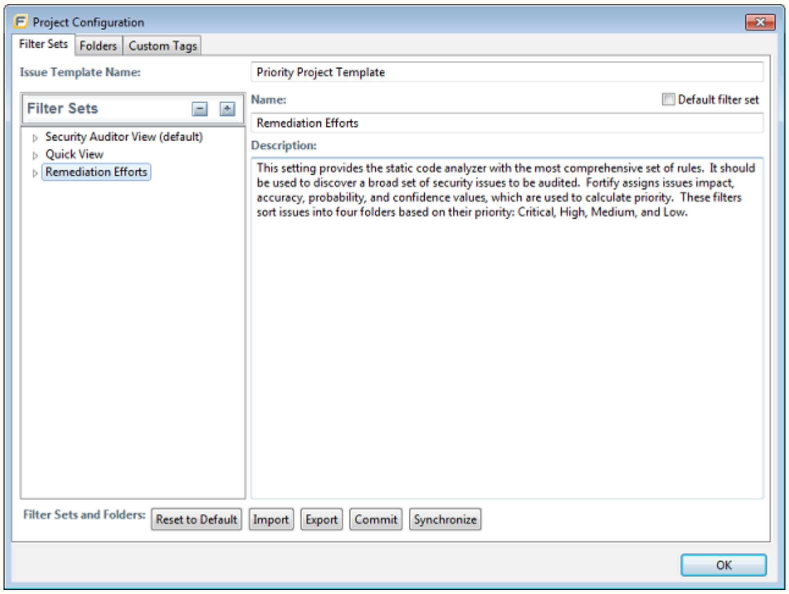
Answer

A Filter Set can be defined with Filters to group and display the findings associated with the different remediation efforts defined by Fortify SCA.

Chapter 4 of the HPE Fortify Audit Workbench User Guide covers Scan Results and it contains a section on *Configuring Custom Filter Sets and Filters.*

Follow the steps in the Audit Workbench User Guide on *Creating a New Filter Set:*

1. Select **Tools > Project Configuration**.
2. Click the **Filter Sets** tab.
3. Next to **Filter Sets**, click **Add Filter Set** ➕ **-** The Create New Filter Set dialog box opens.
4. Type a name for the new filter set (Remediation Efforts)
5. Select an existing filter set to copy (Use Security Auditor View so all issues are included)
6. Click **OK**.



Issue Template Name: Priority Project Template

Name: Remediation Efforts

□ Default filter set

Description:

This setting provides the static code analyzer with the most comprehensive set of rules. It should be used to discover a broad set of security issues to be audited. Fortify assigns issues impact, accuracy, probability, and confidence values, which are used to calculate priority. These filters sort issues into four folders based on their priority: Critical, High, Medium, and Low.

A new filter set with the same folders, visibility filters, and folder filters as the copied filter set is created.

Next, follow the steps in the Audit Workbench User Guide on *Creating a Filter from the Issue Auditing View:*

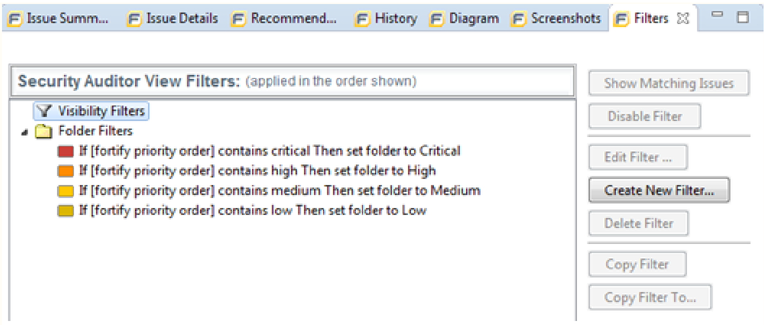
Use the **Filters** tab in the Issue Auditing view to create folder filters for the remediation efforts.

To create a new filter on the **Filters** tab:

1. From the **Filter Set** list (top left of Audit Workbench, below the Summary button), select the filter set created above (Remediation Efforts).
2. Click the **Filters** tab in the Issue Auditing view:

HPE Fortify Version	16.11 and later
Programming Language	□ C/C++ □ .NET □ Java □ Objective-C □ Other
Fortify Audit Workbench	☑ Yes □ No
Fortify IDE Plugin	☑ Yes □ No
Other Fortify Component	□ Yes □ No

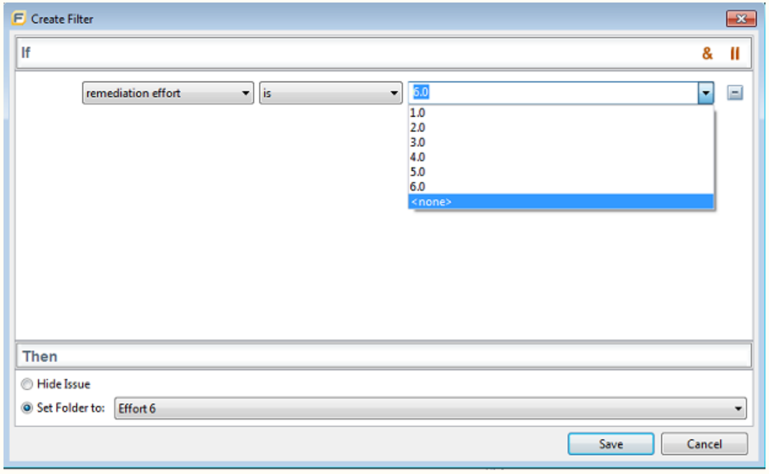
Request code review tools, validations, and support HERE.



Security Auditor View Filters: (applied in the order shown)

- Visibility Filters
- Folder Filters
  - 🟥 If [fortify priority order] contains critical Then set folder to Critical
  - 🟧 If [fortify priority order] contains high Then set folder to High
  - 🟨 If [fortify priority order] contains medium Then set folder to Medium
  - 🟨 If [fortify priority order] contains low Then set folder to Low

3. Right-click **Folder Filters,** and then select **Create New Filter...**
4. From the first list, select the attribute, **remediation effort**
5. From the second list, select **is.**
6. From the third list, select one of the remediation effort levels (only the remediation effort levels that have corresponding findings in the FPR will be shown).



If

remediation effort | is | 6.0

Then

○ Hide Issue

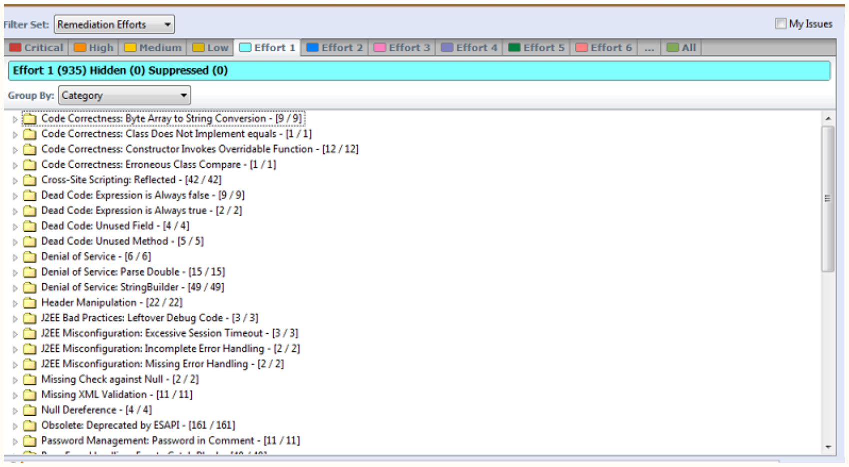
● Set Folder to: Effort 6

7. In the **Then** section, select **Set Folder to:** and select **Other Folder...**
8. Enter a Name to match the remediation effort level chosen in step 6 and choose a unique color for the folder.
9. Click **Save.**

The new filter is displayed at the end of the list. Folder filters are applied in order and the issue is directed to the last folder filter it matches in the list. Issues that match the remediation effort selected will appear in the created folder.

Create a filter for each remediation effort level listed in Step 6 to show all issues reported under their corresponding remediation effort (Repeat steps 3 through 9 for each remediation effort level listed)

The issues will not be shown in the Fortify Priority Order as originally shown, but will instead be shown under the remediation effort level folders created. Note that selecting the Security Auditor View as the Filter Set shows the findings in the original Fortify Priority Order folders.



Filter Set: Remediation Efforts

Effort 1 (935) Hidden (0) Suppressed (0)

Group By: Category

- Code Correctness: Byte Array to String Conversion - [9 / 9]
- Code Correctness: Class Does Not Implement equals - [1 / 1]
- Code Correctness: Constructor Invokes Overridable Function - [12 / 12]
- Code Correctness: Erroneous Class Compare - [1 / 1]
- Cross-Site Scripting: Reflected - [42 / 42]
- Dead Code: Expression is Always false - [9 / 9]
- Dead Code: Expression is Always true - [2 / 2]
- Dead Code: Unused Field - [4 / 4]
- Dead Code: Unused Method - [5 / 5]
- Denial of Service - [6 / 6]
- Denial of Service: Parse Double - [15 / 15]
- Denial of Service: StringBuilder - [49 / 49]
- Header Manipulation - [22 / 22]
- J2EE Bad Practices: Leftover Debug Code - [3 / 3]
- J2EE Misconfiguration: Excessive Session Timeout - [3 / 3]
- J2EE Misconfiguration: Incomplete Error Handling - [2 / 2]
- J2EE Misconfiguration: Missing Error Handling - [2 / 2]
- Missing Check against Null - [2 / 2]
- Missing XML Validation - [11 / 11]
- Null Dereference - [4 / 4]
- Obsolete: Deprecated by ESAPI - [161 / 161]
- Password Management: Password in Comment - [11 / 11]

The template with the Remediation Efforts Filter Set and Folders created can be exported for use with other scans if desired.

From **Tools > Project Configuration,** select **Export** to save the template.

Select **Import** to use the template with other scan results loaded into Audit Workbench.

If the FPR is saved with the Remediation Efforts filter set defined, when the FPR is re-opened in Audit Workbench, the Remediation Efforts filter set will still be available for view.

References

- HPE Fortify Static Code Analyzer User Guide
- HPE Fortify Audit Workbench User Guide